MAY 2 3 2005

SIPRNET CONNECTION GUIDANCE

The Defense Information System Network (DISN) is the mandated DOD component for providing a worldwide network to exchange information in a seamless, interoperable and global battle space. The long-haul telecommunications segment of the infrastructure, which includes the communication systems and services between a fixed environment and the deployed task force, is the primary responsibility of the Defense Information Systems Agency (DlSA). The DISN infrastructure is an integrated network, centrally managed and configured to provide dedicated telecommunications services.

DISA is the connection approval authority for ALL DISN connections. The mission of its SIPRNet Connection Approval Office (SCAO) is to ensure that: Operational requirements have been validated; Connections meet all technical and interoperability requirements; and Sub networks, systems and other connected components provide adequate security and have been accredited by the proper authority.

The SECRET Internet Protocol Router Network (SIPRNet) is just one of the many DISN solutions, operated at the SECRET level for DOD use. Contractors / non-DOD agencies operating on the network must support the DOD mission and comply with DOD IA practices. The Defense agency with a valid classified contract is responsible for submitting the necessary paperwork to get validation from the Joint Staff and approval from OSD to sponsor their contractor(s) for SIPRNet access and for sending the Disclosure Authorization (DA) to obtain approval from other agencies to allow the contractor access to their information DISA then uses the Internet Protocol(IP) addresses supplied by the agencies on the DA form to build the filters for the contractors that effectively says "You can go where the DA says and nowhere else".

Several terms are associated with the SIPRNet process:

1. Authority to Operate (ATO) - DSS' acceptance of risk for operations and definition of the accreditation boundaries.
2. Interim Approval to Connect (IATC) - Defines the contractor's connection boundaries as accepted by DISA.
3. Consent to Monitor (CTM) - Declaration that DlSA can access the contractor's network infrastructure. All enclaves connected to the DISN long haul are subject to compliance inspections.
4. SIPRNet Connection Questionnaire (SCQ) - Provides specific network infrastructure information.
5. Network Diagram - The topology reflects all devices connected physically or logically to the local classified infrastructure.
6. Authority to Connect (ATC) - Defines the contractor's connection boundaries as accepted by DISA after successful completion of a network vulnerability assessment.

The SIPRNet connection process provided here is intended to allow you to organize your thoughts when SIPRNet access is required, to answer general questions about access and to give you a ready contact reference for the difficult questions. This is a partnership of DSS, the sponsor and the contractor. Each has a role to do in bringing the system to operational readiness. If you have suggestions for how the process can be improved within the guidelines of the laws and policy, please send them to DISN@dss.mil.

Reference: CJCSI6211.02B
00015200.40
0001 5220.22-M

Attachment
1. SIPRNet Contractor Accreditation Process (SCAP) (Industry Only)